PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-256746
(43)Date of publication of application : 12.09.2003

(51)Int.Cl. G06F 17/60
B42D 15/10
G06K 17/00
G06K 19/00
G06K 19/10
G06T 1/00
G06T 7/00
G07F 7/12
H04L 9/32

(21)Application number : 2002-052670
(22)Date of filing : 28.02.2002

(71)Applicant : OMRON CORP
(72)Inventor : KOJI RYOICHI

(54) TRANSACTION PROCESSING DEVICE, TRANSACTION PROCESSING SYSTEM, AND TRANSACTION PROCESSING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent an illegal use of a credit card more effectively than in a conventional method.
SOLUTION: A CAT (credit authorization terminal) 1 is provided with a card reader part 9 reading face image data from the card, a face feature point extraction part 14 for extracting feature points from the face image data read by the card reader part 9 as feature point data, a communication circuit 13 for sending the feature point data extracted by the face feature point extraction part 14 to a host computer 3, and a display part 10 for displaying the face image data read by the card reader part 9 and results of certification sent from the host computer 3.

LEGAL STATUS

[Date of request for examination] 15.11.2004
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－256746
（P2003－256746A）
(43)公開日　平成15年９月12日(2003.9.12)

(51)Int.Cl.⁷	識別記号	FI		テーマコード(参考)
G06F 17/60	414	G06F 17/60	414	2C005
	402		402	3E044
	510		510	5B035
B42D 15/10	501	B42D 15/10	501B	5B057
	521		521	5B058

審査請求　未請求　請求項の数４　ＯＬ　（全 11 頁）　最終頁に続く

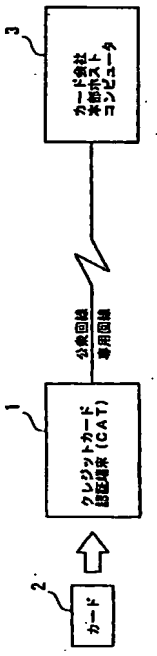
(21)出願番号　特願2002－52670(P2002－52670)
(22)出願日　平成14年２月28日(2002.2.28)

(71)出願人　000002945
オムロン株式会社
京都市下京区塩小路通堀川東入南不動堂町801番地
(72)発明者　興治　良一
京都府京都市下京区塩小路通堀川東入南不動堂町801番地　オムロン株式会社内
(74)代理人　100085006
弁理士　世良　和信　（外１名）

最終頁に続く

(54)【発明の名称】　取引処理装置、取引処理システムおよび取引処理方法

(57)【要約】
【課題】　クレジットカードの不正使用をより効果的に防止すること。
【解決手段】　カードから顔画像データを読み取るカードリーダ部９と、カードリーダ部９により読み取られた顔画像データから特徴点を特徴点データとして抽出する顔面特徴点抽出部１４と、顔面特徴点抽出部１４により抽出された特徴点データをホストコンピュータ３に送信する通信回路１３と、カードリーダ部９により読み取られた顔画像データの表示、およびホストコンピュータ３から送信された認証結果を表示する表示部１０と、を備えたＣＡＴ１。



1

【特許請求の範囲】
【請求項１】カードから顔画像データを読み取る読取手段と、
前記読取手段により読み取られた顔画像データから特徴点を特徴点データとして抽出する特徴点抽出手段と、
前記特徴点抽出手段により抽出された特徴点データをセンタ装置に送信する送信手段と、
前記読取手段により読み取られた顔画像データの表示、および前記センタ装置から送信された認証結果を表示する表示手段とを備えた取引処理装置。
【請求項２】カードから顔画像データを読み取る読取手段と、
前記読取手段により読み取られた顔画像データから特徴点を特徴点データとして抽出する特徴点抽出手段と、
前記特徴点抽出手段により抽出された特徴点データを送信する送信手段と、
前記読取手段により読み取られた顔画像データの表示、および前記特徴点データに基づいた認証結果を表示する表示手段と、を備えた取引処理装置と、
前記取引処理装置から前記特徴点データが送信され、送信された前記特徴点データに基づいて認証を行う認証手段を備えたセンタ装置と、
からなる取引処理システム。
【請求項３】前記カードの利用が正規ユーザによる利用かどうかの判定を一定の閾値を基準にして判定する請求項２記載の取引処理システム。
【請求項４】カードから顔画像データを読み取り、
顔画像データから特徴点を抽出し、
抽出された特徴点をセンタ装置に送信し、
顔画像データに基づいて顔画像およびセンタ装置から送信された認証結果を表示する取引処理方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はクレジットカードの不正使用を防止する取引処理技術に関する。
【０００２】
【従来の技術】クレジットカード（以下特に断らない限り「カード」という。）は現金を持ち歩かなくても買物ができるという利便性から普及し、今日、キャッシュレス社会を実現するまでにいたっている。
【０００３】しかしながらクレジットカードを利用した不正が後を絶たない。このため、クレジットカード会社は、加盟店にクレジットカード認証端末であって取引処理装置として機能するＣＡＴ(クレジット・オーソライゼーション・ターミナル）を設置してもらい、顧客が提示したカードが不正使用されていないか否かをその場で判定する防犯システムを採用している。
【０００４】
【発明が解決しようとする課題】カードを紛失したり盗難にあったりした場合、最寄りの警察やカード会社に連絡し、自己所有のカードの利用を差し止めて他人による不正使用を防止するようになっているけれども、紛失や盗難にあったことをすぐには気付かない場合がある。

2

【０００５】その場合、被害届けが出される前に第三者による不正使用がなされると、ＣＡＴを用いた防犯システムを採用していても回避できない場合が少なくない。
【０００６】周知のごとくカードを利用するにあたり、利用者は伝票にサインし、加盟店側ではカードに記載された正規ユーザによる自署と一致するか否かをチェックするようにはなっている。しかしながら、確信がない以上、不正の有無を客側に問い質すことは、正規ユーザによるカード利用であったことを考慮すると店のイメージダウンにも繋がるため多くはない。
【０００７】また、正規ユーザの顔の特徴点をカードに記憶させておき、カード利用者の不正をチェックするシステムが採用されているが、利用者の顔から特徴点を認識するには、その利用者の顔を店員が注視する必要があり、やはり店のイメージダウンにつながる。
【０００８】このため不審なカード利用者とは思ってもカードの利用を許諾してしまう加盟店も少なくなく、よってカード会社が損害を補償するケースが後を絶たない。
【０００９】クレジットカード会社では、カード表面に本人の写真を貼りつけるなどして防犯に努めているが、写真が張り替えられてしまう虞がある。
【００１０】そこで、顔写真データをクレジットカード会社のホストコンピュータに送信して照合するシステムが知られているが、通信中に顔写真データが盗まれてしまうと偽造される虞がある。
【００１１】本発明は、上記実情に鑑みてなされたものであり、その解決しようとする課題は、カードの不正使用を従来よりも効果的に防止できる技術を提供することにある。
【００１２】
【課題を解決するための手段】本発明は、前述の技術的課題を解決するために以下のようにした。
【００１３】すなわち、本発明は、カードの内部メモリに正規ユーザの顔面特徴点データを記録しておく。またクレジットカード会社のホストコンピュータには正規ユーザ判定用に顔面特徴点データをデータベース化しておく。
【００１４】また当該カードを利用するとＣＡＴ上のディスプレイに正規ユーザの顔が表示されるようになっている。よって、正規ユーザによるものか不正な使用者によるものか確認できる。
【００１５】さらにＣＡＴでカードを読み取ると、正規ユーザの顔面特徴点データが抽出される。また、クレジットカード会社のホストコンピュータにはクレジット利用データが送信される。
【００１６】送信された情報が、ホストコンピュータに

記録されている正規ユーザの顔面特徴点データと一致した場合、ホストコンピュータはカード利用者を正規ユーザと特定し、当該カードは正当に利用されているというメッセージをＣＡＴの表示部に出す。

【００１７】なお、ＣＡＴ自体にまたはその近傍の店内適所に例えば電子スチルカメラを装備しておき、利用者を撮影する。そして、その生の顔写真データをホストコンピュータに送信し、ホストコンピュータで受信したカード利用者の顔から特徴点を抽出する。この抽出された特徴点を、現在、カードを利用している者の顔面特徴点データとし、当該データをホストコンピュータに記録されている正規ユーザの顔面特徴点データと照合するようにしてもよい。

【００１８】よって不正使用の防止を強化できる。

【００１９】さらにセキュリティを高められるように前記抽出した顔面特徴点データにスクランブルをかけることもできる。

【００２０】顔面照合の代わりに、指紋照合やアイリス照合等に置き換えてもよい。

【００２１】ホストコンピュータの真偽判定運用に関しては、一定の閾値を設定し、照合による一致程度が0～60%の場合は無条件にカードの利用を拒絶するようにし、61～80%の場合は不審客として通信手段等の他の確認手段を用いた判定を行ってからカードの利用の可否を行うようにし、81～100%の場合は正規ユーザによる正規なカードの利用が為されているという判定を行うようにすることも考えられる。閾値はパラメータとして運用に応じて変更すると好適である。なお、ホストコンピュータとの間での通信途中に万一特徴点データが盗まれたとしても特徴点だけで正規利用者の顔を復元することは不可能である。よってセキュリティの向上を期待できる。

【００２２】

【発明の実施の形態】以下、本発明の実施の形態（以下「実施形態」という）を図示例と共に説明する。

【００２３】図１に本発明に係るクレジットカードを利用した商品購入のシステム構成の概略図を示す。

【００２４】符号１，２および３は、それぞれＣＡＴ，クレジットカードおよびクレジットカード会社の本部（センタ）に設置されたホストコンピュータ（センタ装置）を示す。

【００２５】ＣＡＴ１とクレジットカード会社のホストコンピュータ３とは、公衆回線や専用回線を通じて繋がっている。そして、クレジットカード（以下「カード」という。）２をＣＡＴ１で読み込むとカード２に記憶されている各種情報がホストコンピュータ３に電送される。

【００２６】次に図２および図３を用いてカード２の構成を示す。

【００２７】図２にはカード２の表面に刻まれた各種カード情報（カード表面情報）を示す。カード情報として、例えば正規ユーザ（所有者）のＩＤ番号，カード所有者の氏名，カードの有効期限，所有者の顔写真等がカード表面に記載される。これらの情報のうち例えばＩＤ番号，本人の氏名，カードの有効期限等は、オフライン運用を図るためにエンボス化してある。

【００２８】また、図３はカード２の内部メモリに記憶されている情報の例示である。当該メモリ記憶情報としては例えばカード所有者のＩＤ番号，カード所有者の氏名，カードの有効期限，カード所有者の顔画像データ（当該顔画像データがあればカード所有者の顔をＣＡＴ１やホストコンピュータのディスプレイに正確に表出することができる。顔画像データには正規カード所有者の顔の特徴部分についての情報が少なくとも含まれる。なお当該特徴部分の情報を顔面特徴点データということにする。）をデータ化し記憶してある。顔画像データは、デジタル画像として処理される。なおクレジットカードはＩＣカードその他のメモリー媒体方式のカードでも適用できる。

【００２９】顔画像データは、カード発行時にカード所有者本人の顔を撮影し、かつこれをデータ化したものである。よって、顔画像データのことを写真データという場合がある。またホストコンピュータ３にも顔画像データや顔面特徴点データが格納される。

【００３０】次に図４および図５を参照して、クレジットカード２とＣＡＴ１とホストコンピュータ３との関係を説明する。

【００３１】なお、図４に示す（Ｉ）～（ＩＩ）の符号および図５に示す（Ｉ）～（ＩＩ）の符号は、同一の符号同士で対応しており、処理の移行先を案内する。例えば、図４の（Ｉ）は、図５の（Ｉ）と対応しており、図４の（Ｉ）に係るルートにおける処理は、図５の（Ｉ）に係るルートに移行してそのまま図５で続行されることを意味する。図面についてのこのような対応関係は図６と図７、および図８と図９においても適用される。

【００３２】ＣＡＴ１は、クレジットカード２が有する各種情報を読み取る読取手段としてのカードリーダ部９と、カード表面の顔面写真を表示したり、ＣＡＴ６のオペレータに種々の指示をしたり各種情報を表示したりする表示手段としての表示部１０と、買物金額等を入力するためのテンキー部１１と、カードで購入した商品の支払方法について一括払いか分割払か（クレジット金額支払処理区分）の選択をするファンクションキー部１２と、カード２から読み取った利用者のＩＤ情報や顔面特徴点データをホストコンピュータ３に送受信するための送・受信手段としての通信回路１３と、カードリーダ部９によりカード２から情報として読み取った顔面写真からバイオメトリックス技術によって正規ユーザの顔面の特徴点を抽出するための顔面特徴点抽出手段としての顔面特徴点抽出部１４と、データを暗号化するための暗号

5

化回路１５と、ＣＡＴ３を構成する各部に直流電圧を供給する電源回路１６と、プリンタ制御部２１と、プリンタ制御部２１の制御によりクレジット伝票を印刷したり、一日のクレジット売上げ集計を印字したりするプリンタ部２２と、ＣＡＴ全体を制御する制御部２４を有する。

【００３３】カード会社のホストコンピュータ３は、各店舗に設置してあるＣＡＴ１から送信されてくる暗号化された各種データを受け取り、各加盟店に設置してあるＣＡＴ１との間でクレジット承認ジョブを実施する通信部１７と、通信部１７で受け取った暗号化データを解読してもとの値に戻す（解凍する）暗号解読部１８と、正規ユーザの前記各種データを予め登録してあるデータベースファイル部１９と、データベースファイル部１９内の該当者のデータおよび前記暗号解読部１８によって解読したデータとを比較判定する判定指示部２０と、カード２の利用が正規ユーザによる利用か不正使用者による利用であるかの照合を行うために用いられる閾値を設定する閾値設定部２３と、ホストコンピュータ全体を制御する中央演算処理装置であるＣＰＵ部２５を有する。

【００３４】ホストコンピュータ３の暗号解読部１８は、前もって収蔵してあるクレジットカード会員のデータからＩＤ番号を枕として顔面特徴点データを引き出し、以前同一カードを利用して商品の購入を行った際になされたＣＡＴ１から得た先の通信に基づくデータとの突き合わせを行う。

【００３５】顔面の特徴点照合判定を行うに際し、閾値設定部２３ではバイオメトリックス技術判定を行う。その関係で100%完全な一致をみるには無理がある。よって、閾値のレベルに応じて真偽判定を決める。例えば照合による一致程度が0～60%の場合は無条件にカードの利用を拒絶し、61～80%の場合は不審客として電話その他の通信手段を用いた判定を併用し、その結果をまってカード利用の可否を行い、81～100%の場合は正規ユーザによる正規なカード利用が為されているという判定を行う。

【００３６】なお、図中の実線矢印は、クレジットカード２，ＣＡＴ１およびホストコンピュータ３相互において、各種情報や命令の送受信を行うことを目的として、ＣＡＴ１およびホストコンピュータ３それぞれの構成部同士を連結する配線（バス）やＣＡＴ１およびホストコンピュータ３を結ぶ通信経路を示す。また、破線矢印は、クレジットカード２に含まれている正規データが、ＣＡＴ１のデータベースファイル部１９にも記憶され相互にリンクしていることを意味する。

【００３７】本システムにあっては、矢印１００は、カード利用者がＣＡＴのオペレータに差し出すことを示唆する。差し出されたカード２は、ＣＡＴ１のカードリーダ部９で読み込まれてＣＡＴ内部に取り込まれる。

【００３８】また、矢印１０４は、ＣＡＴ１およびホストコンピュータ３を結ぶ前記通信経路であり、ＣＡＴ１とホストコンピュータ３とが、それぞれの通信手段（ＣＡＴ１の場合は通信回路１３であり、ホストコンピュータ３の場合は通信部１７である。）により、公衆回線や専用回線を通じて繋がっていることを示す。

6

【００３９】カードリーダ部９で読み取られたクレジットカード２に含まれている、ＩＤ番号，カード所有者の氏名，カードの有効期限，カード所有者の顔写真，当該所有者の顔画像データのデータ，テンキー入力部１１で入力された買物金額等のデータ，クレジット金額支払処理区分等ファンクションキー部１２で選択されたデータは、制御部２４に送られる（矢印１０６，１０８，１１０参照）。

【００４０】制御部２４に送られた情報のうち所有者の顔画像データである写真データは、顔面特徴点抽出部１４を経由して（矢印１１２参照）暗号化回路１５に送られる（矢印１１４参照）。

【００４１】暗号化回路１５で暗号化されたデータやテンキー部１１およびファンクションキー部１２による入力データは、通信回路１３を経由して通信回路１３に送られ（矢印１１６，１１７参照）、その後ホストコンピュータ３の通信部１７に送信される（矢印１０４参照）。

【００４２】暗号化するためのキーは、ホストコンピュータ３側から変更可能である。また、万一ＣＡＴ１が盗難にあい、窃盗犯が写真データから正規ユーザの顔についての特徴点を抽出しようと試みても、顔面特徴点データは得られないようになっている。さらに暗号化回路のキーは不定期に変更できるようにしてあり、仮に解読したとしても暗号化のアルゴリズム等が変わるようになっている。このため、同じキーを店舗に設置してあるＣＡＴ１からデータ送信することはできない。

【００４３】また、制御部２４に送られた各種データに基づいて、表示部１０には必要情報が表示される。

【００４４】ＣＡＴ１から送信されたデータは、通信部１７を経由して暗号解読部１８に送られる（矢印１０４，１２６参照）。そして、暗号解読部１８によって解読されたデータは、ＣＰＵ部２５に送信され、そこで必要な演算処理を実行してから通信部１７，閾値設定部２３，判定指示部２０に送られる（矢印１２８、１３０，１３４，１３６参照）。また、ＣＰＵ部２５とデータベースファイル部１９との間では、相互にデータのやり取りが行われる（矢印１３２，１３８参照）。

【００４５】判定指示部２０による判定結果は、通信部１７に送られ（矢印１４０参照）、その後ＣＡＴ１の通信回路１３に公衆回線や専用回線を通じて送られる（矢印１４０，１０４参照）。

【００４６】前記判定結果とは、例えば、カードユーザのブラックリストチェックやカードの有効期限チェックなどを行った結果ホストコンピュータ３でカード利用が

正当か否かの判定内容や正規ユーザの写真データの表出を例示できる。

【００４７】通信回路１３を経由してＣＡＴ１に入った判定結果は、制御部２４を経由して表示部１０に表示される。表示部１０に表示された内容によりオペレータは正規ユーザによる有効なカード利用であるか否かがわかる。

【００４８】そして、正規ユーザによる有効なカード利用であることが判明し、カード２の有効性について確認が取れた場合、ＣＡＴ１はその制御部２４によりプリンタ制御部２１を経由してプリンタ部２２を作動させ、伝票を印刷する（矢印１１８，１２０参照）。

【００４９】次に図６および図７のフローチャートを参照して本システムの流れを説明する。

【００５０】本システムは、以下に述べるステップ１０１～ステップ１２０からなる。なおステップを例えばＳ１０１と記号Ｓを用いて表記する。

【００５１】Ｓ１０１では、カード２を利用して買物等を行いたいと思う顧客が加盟店の店員にその旨を告げると、店員はカード利用者である顧客からカード２を受け取り、ＣＡＴ１によるクレジット売上げ承認の手続の開始をオペレータとして実行する。

【００５２】Ｓ１０２では、オペレータである店員が、カード２に表示されている写真とカード利用者とが同一人であるかをまず目視確認する。そして、同一人と判断（肯定判定）すればＳ１０３に進み、別人と判断（否定判定）すればＳ１０４に進む。フローチャートでは、等記号を用いた”カード写真＝本人顔？”という表記で判定を実行することを示す。

【００５３】Ｓ１０３では、店員は商品の値段である売上金額やその支払回数をどうするかについて顧客に問い合わせ、その内容をテンキー入力部１１やファンクションキー部１２の操作によって入力する。

【００５４】Ｓ１０５ではカードリーダ部９でクレジットカード２の読み取りを行い、カード２が有する前記各種情報がＣＡＴ１に取り込まれる。

【００５５】Ｓ１０６ではカード２の内部メモリに記憶した正規ユーザの顔面特徴点データが読み取られ、ＣＡＴ１の表示部１０に正規ユーザの顔面が表示される。

【００５６】Ｓ１０９ではホストコンピュータ３の通信部１７を経由してホストコンピュータ３に顔面特徴点データを送信する。

【００５７】Ｓ１１０では、ホストコンピュータ３で判定を行う。

【００５８】Ｓ１１１では、ホストコンピュータ３の通信部１７を経由してホストコンピュータ３の判定結果をＣＡＴ１に送信する。

【００５９】Ｓ１１２では、ホストコンピュータ３の通信部１７を経由してホストコンピュータ３の判定結果をＣＡＴ１の表示部１０に表示する。判定結果は前記閾値

による一致程度が幾らであるかで決定する。一致程度が0～60％の場合は無条件にカードの利用を拒絶する。すなわち判定はＮＧとなる。一致程度が0～60％以外の場合は、正規ユーザによる利用がなされていると判断されたか、またはどちらか不明であるという判断がされたことになる。

【００６０】Ｓ１１２で否定判定した場合はＳ１１３に進み、肯定判定した場合は、Ｓ１０４に進む。

【００６１】Ｓ１１３では一致程度が0～60％の場合でないことを前提に一致程度が61～80％か否かを判定する。Ｓ１１３で否定判定した場合はＳ１１５に進み、肯定判定した場合は、Ｓ１１６に進む。Ｓ１１３では、この内容を”判定グレー？”と表記する。

【００６２】Ｓ１１５では一致程度が0～80％でない場合、すなわち一致程度が81～100％の場合であるから正規ユーザによるカードの利用と判定され取引が成立する。

【００６３】Ｓ１１７ではプリンタ制御部２１の制御によりプリンタ部２２を作動してクレジット伝票の発行をする。

【００６４】Ｓ１１８では顧客であるカード利用者に伝票へのサインを依頼し、Ｓ１２０で本システムによる取引を終了する。なお、取引がなされたことの証拠として、カード利用者にはカード裏面に記入されているサインと同じ形態のサインを伝票に記入してもらい、これをもって取引が成立する。当該取引データは、ＣＡＴ内部にタンキングされる。そして、閉店時や営業時間中の指定時間中にホストコンピュータ３に取引トランザックションデータとして送信される。

【００６５】Ｓ１１３で肯定判定した場合に進むＳ１１６ではカード利用者が正規ユーザか否か不明であるので、コンピュータによる判定ではなく人による再度の判定を行う。この内容を”取引有人再確認”と表記する。この判定を行うのにＳ１１９でクレジットカード会社の例えば電話センタに連絡する。

【００６６】Ｓ１１９の次はＳ１１４に進む。Ｓ１１４では、Ｓ１１３と同様”判定がグレーか否かを判定し、否定判定した場合はＳ１１５に進み、肯定判定した場合はＳ１０４に進む。

【００６７】なお、ＣＡＴ自体にまたはその近傍の店内適所に例えば電子スチルカメラを装備しておき利用者を撮影する。そして、ＣＡＴ１から生の顔写真データをホストコンピュータ３に送信し、ホストコンピュータ３で顔の特徴点を抽出し、ホストコンピュータ３に格納してある顔面特徴点データと突き合わせるようにしてもよい。

【００６８】次にこのような構成の本システムを利用したクレジットカードの不正使用防止技術の作用効果を述べる。

【００６９】〈第一の不正防止効果〉本システムにあって

は、カード２内に従来のクレジット利用に不可欠なＩＤ等のデータに加え正規ユーザの顔面の写真データが記憶される。そして、ホストコンピュータ３ではその写真データから、カード表面上からは一切判明しない正規ユーザ判定用の顔面特徴点データを別途抽出する。また顔面特徴点データはデジタル化されてホストコンピュータ３のデータベースファイル部１９に前記ＩＤその他の個人情報と合わせて記憶されている。

【００７０】よって、正規の利用者がカード２を利用すると、ＣＡＴ１上の表示部１０にカード２の内部メモリーから読み取った写真データに基づいた顔写真が表出し、オペレータが正規ユーザによるカード利用の有無を目視で確認できる。この結果、カードの不正防止効果が高まる。

【００７１】〈第二の不正防止効果〉カード２の写真データがＣＡＴ１で読み取られ特徴点が抽出される。抽出されたデータはＣＡＴ１内部の暗号化回路１５により暗号化された顔面特徴点データ(顔画像データ全体ではない)だけでなく前記ＩＤ等の個人データがホストコンピュータ３に送信され正規ユーザであるか否かの本人照合がなされる。

【００７２】なお、ホストコンピュータ３との間での通信途中に万一特徴点データが盗まれたとしても特徴点だけで正規利用者の顔を復元することは不可能である。よってセキュリティの向上を期待できる。

【００７３】そしてホストコンピュータ３に記憶されている正規ユーザの顔画像データおよびホストコンピュータ３に送信されてきた各種データが一致すると、ホストコンピュータ３は利用者が正規ユーザであると判定してカード２の利用が可能であるという内容のメッセージ等をＣＡＴ１の表示部１０に表示する。

【００７４】ホストコンピュータ３に保管されているデータは、部外者が触れることのできない唯一の本人照合キーであることによる不正防止効果を図れる。

【００７５】〈第三の不正防止効果〉カード２が盗難にあってカード２の顔写真がスリ替えられたとしても、ＣＡＴ１の表示部１０には、カード２の内部メモリに記憶されている写真データに基づいた正規ユーザの顔が表示される。この場合、カード２の顔写真とカード２の内部メモリーに記憶されている写真データに基づいて表出される顔とは不一致である。よって、カード２の内部メモリに記憶されているデータが改竄されない限り、ＣＡＴ１のオペレータは正規ユーザによるカード利用か否かを簡単に見分けられる。したがって不正使用は極めて難しくなる。

【００７６】〈第四の不正防止効果〉高等技術の駆使により、盗んだカード２の顔写真をすり替えたり、またはカード２の内部メモリに記憶してある写真データをも入れ替えたりしても、ホストコンピュータ３に記憶されている正規ユーザの写真データと異なるため、カードの不正使用を簡単に発覚できる。

【００７７】〈第五の不正防止効果〉カードでなくＣＡＴ１が盗難されて盗難カードが擦られ、その内部メモリに不正使用をしようとする者の写真データがたとえ記憶されたとしても、ホストコンピュータ３に記憶されている正規ユーザの写真データが改竄されない限り、不正使用はできない。

【００７８】〈第六の不正防止効果〉さらにセキュリティを高められるようにするために、カード２上の顔面データ読取時に暗号化回路１５を通して抽出した顔面特徴点データにスクランブルをかけることも考えられる。

【００７９】この場合、不定期に暗号化のアルゴリズムが変更されるので暗号化された特徴点はもとのオリジナルの特徴点を特定できない。よって、カードの不正使用を有効に防止できる。

【００８０】（変形例）顔面写真で照合する代わりに指紋で照合するようにしてもよい。

【００８１】この場合、写真データの代わりに正規ユーザの指紋をデータ（以下「指紋データ」）として取り扱うようにし指紋データを解読し、ホストコンピュータに記憶してあった正規ユーザの指紋データと突き合わせるようにする。よってシステム上、カード２の内部メモリに指紋データを記憶する点，ＣＡＴ１の顔面特徴点抽出部１４が図示しない指紋特徴点抽出部になる点，ホストコンピュータ３のデータベースファイル部１９に正規ユーザの指紋データが記憶される点が、写真データを用いる場合と相違する。

【００８２】また、図８および図９は指紋照合を行う場合のフローチャートを示す。

【００８３】このフローチャートが図６および図７のフローチャートと相違する点は、図６および図７のフローチャートに係るＳ１０６，Ｓ１０７，Ｓ１０８およびＳ１１２がそれぞれ、Ｓ２０６，Ｓ２０７，Ｓ２０８およびＳ２１２に変更された点と、Ｓ１０６およびＳ１０７にそれぞれ対応するＳ２０６およびＳ２０７の処理順序が前後する点である。よって、図６および図７のフローチャートと同一部分には同一符号を付して説明を省略する。

【００８４】図８において、Ｓ１０５の次に進むＳ２０７では、カード２の内部メモリに記憶してある指紋データが正規ユーザの指紋か否かを判定する。肯定判定した場合は、Ｓ２０６に進み、否定判定した場合はＳ１０４に進む。

【００８５】前記判定は等記号を用いて”カード内指紋データ＝本人指紋？”と表記する。

【００８６】Ｓ２０７で肯定判定した場合に進むＳ２０６では、カード２の内部メモリに記憶した正規ユーザの指紋データが読み取られ、ＣＡＴ１の表示部１０に正規ユーザの指紋照合が適正である旨を表示する。

【００８７】Ｓ２０８では、当該カード２に記憶されて

ある指紋データを前記指紋特徴点抽出部により抽出し、その後暗号化回路によって抽出した指紋特徴データを暗号化する。

【００８８】Ｓ２１２では、ホストコンピュータ３の通信部１７を経由してホストコンピュータ３の判定結果をＣＡＴ１の表示部１０に表示する。判定結果を閾値による一致程度が幾らであるかで決定するのは顔面特徴点データの場合と同じである。一致程度が0～60%の場合は無条件にカードの利用を拒絶する。すなわち判定はＮＧとなる。一致程度が0～60%以外の場合は、正規ユーザによる利用がなされていると判断されたか、またはどちらか不明であるという判断がされたことになる。

【００８９】Ｓ２１２で否定判定した場合はＳ１１３に進み、肯定判定した場合は、Ｓ１０４に進む。

【００９０】なお、顔面特徴点データや指紋データの代わりに周知のアイリス照合でも適用することが考えられる。

【００９１】（応用例）顔面特徴点データ，指紋データ等の適用技術の応用例として次のような場合が考えられる。

【００９２】顔写真を内部メモリーに記憶した身分証明カードを警備員に発行する。そして、警備員が規定の業務を遂行しているか否かがわかるよう、巡回先の適所に数箇所カード処理端末を設置する。そして、前記適所に警備員が巡回してきたらカードを読み込ませることで規定の業務を警備員が遂行しているか否かの判定をする。

【００９３】また、銀行の貸金庫への出入口記憶レコーダとしての利用も考えられる。

【００９４】さらに、例えばヘルスセンタ等における複数の商品売場での掛け売り処理を本人の顔画像データ等をキーとして行うことで、ＰＯＳ会計事務処理への適用ができる。

【００９５】さらにまた、ホテル内でのレストラン等での部屋へつけ売りする場合の本人特定用に顔面照合等を適用することも考えられる。

【００９６】加えて、プールでの料金精算にも利用できる。この場合も顔画像データ等をキーとして掛け売り金額をすべてＰＯＳに記憶する。

【００９７】さらに、レンタルビデオ店やレンタカー事務所での本人照合ＰＯＳとして幅広い利用も考えられる。

【００９８】また、車両の盗難防止を図るため、駐車場での運転者特定用のタイムレコーダとしても使える。

【００９９】

【発明の効果】以上、説明したように本発明によれば、クレジットカードの不正使用を従来の技術よりも効果的に防止できる。

【図面の簡単な説明】

【図１】本発明に係るクレジットカードを利用した商品購入のシステムを示す概念図である。

【図２】本発明に係るクレジットカードの表面に記載の情報内容を示す図である。

【図３】本発明に係るクレジットカードの内部メモリに記憶されている情報内容を示す図である。

【図４】クレジットカードを利用した商品購入のシステムを示す概念図である。

【図５】図４に連続した図である。

【図６】本発明に係るクレジットカードを利用した商品購入のシステムを説明するためのフローチャートである。

【図７】図６に連続した図である。

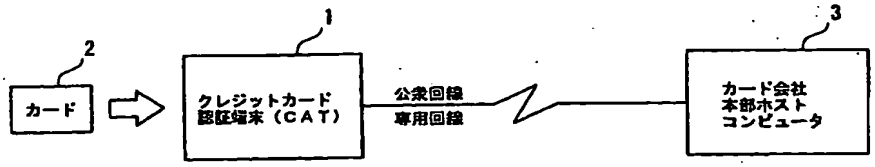
【図８】本発明に係るクレジットカードを利用した商品購入のシステムの変形例を説明するためのフローチャートである。

【図９】図８に連続した図である。

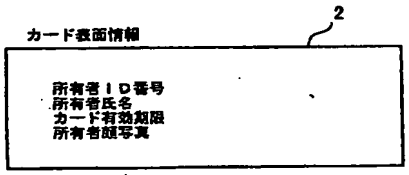
【符号の説明】

１ ＣＡＴ（取引処理装置）
２ クレジットカード
３ ホストコンピュータ（センタ装置）
９ カードリーダ部（読取手段）
１０ 表示部（表示手段）
１１ テンキー部
１２ ファンクションキー部
１３ 通信回路（送信手段）
１４ 顔面特徴点抽出部（顔面特徴点抽出部）
１５ 暗号化回路
１６ 電源回路
１７ 通信部
１８ 暗号解読部
１９ データベースファイル部
２０ 判定指示部
２１ プリンタ制御部
２２ プリンタ部
２３ 閾値設定部
２４ 制御部
２５ ＣＰＵ部

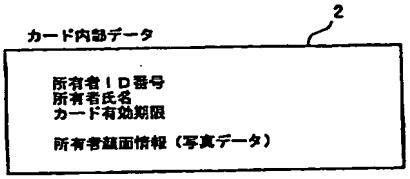
【図１】


2
カード
1
クレジットカード
認証端末（ＣＡＴ）
公衆回線
専用回線
3
カード会社
本部ホスト
コンピュータ

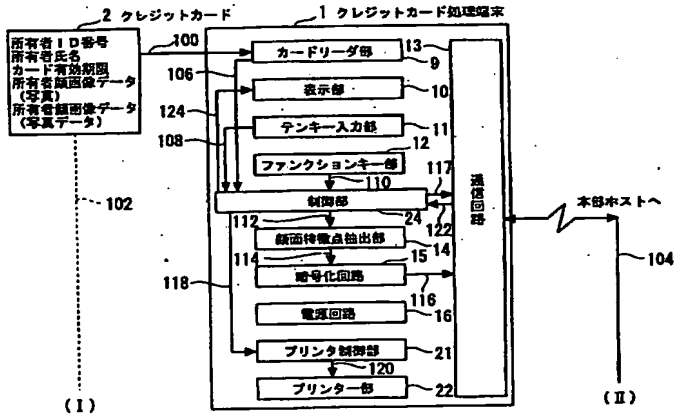
【図２】


カード表面情報
2
所有者ＩＤ番号
所有者氏名
カード有効期限
所有者顔写真

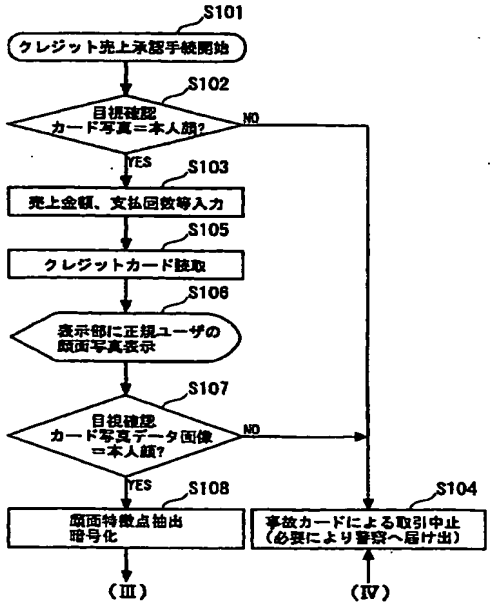
【図３】


カード内部データ
2
所有者ＩＤ番号
所有者氏名
カード有効期限
所有者顔面情報（写真データ）

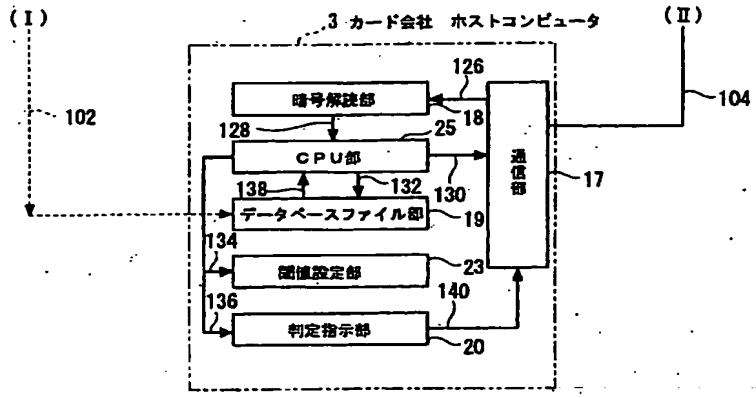
【図４】


2 クレジットカード
1 クレジットカード処理端末
所有者ＩＤ番号
所有者氏名
カード有効期限
所有者顔画像データ（写真）
所有者顔画像データ（写真データ）
100
カードリーダ部
13
9
106
表示部
10
124
テンキー入力部
11
108
ファンクションキー部
12
117
110
制御部
112
24
122
顔面特徴点抽出部
15
14
114
暗号化回路
118
116
電源回路
16
プリンタ制御部
21
120
プリンター部
22
通信回路
本部ホストへ
104
102
（Ⅰ）
（Ⅱ）

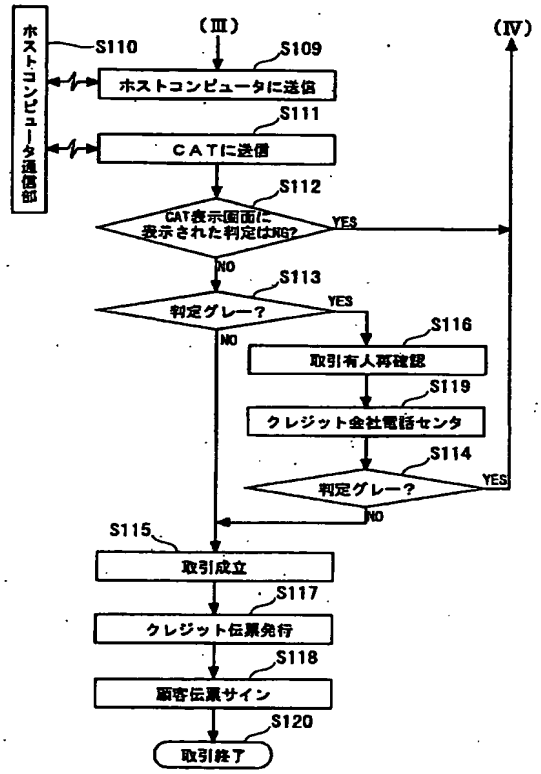
【図６】


S101
クレジット売上承認手続開始
S102
目視確認
カード写真＝本人顔?
NO
YES
S103
売上金額、支払回数等入力
S105
クレジットカード読取
S106
表示部に正規ユーザの顔面写真表示
S107
目視確認
カード写真データ画像＝本人顔?
NO
YES
S108
顔面特徴点抽出
暗号化
S104
事故カードによる取引中止（必要により警察へ届け出）
（Ⅲ）
（Ⅳ）

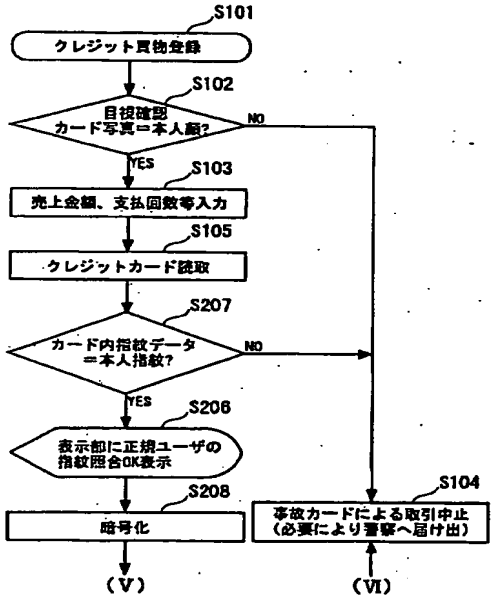
【図５】


(Ⅰ)
3 カード会社 ホストコンピュータ
(Ⅱ)
102
126
暗号解読部
18
104
128
25
CPU部
通信部
17
138
132
130
データベースファイル部
19
134
閾値設定部
23
140
136
判定指示部
20

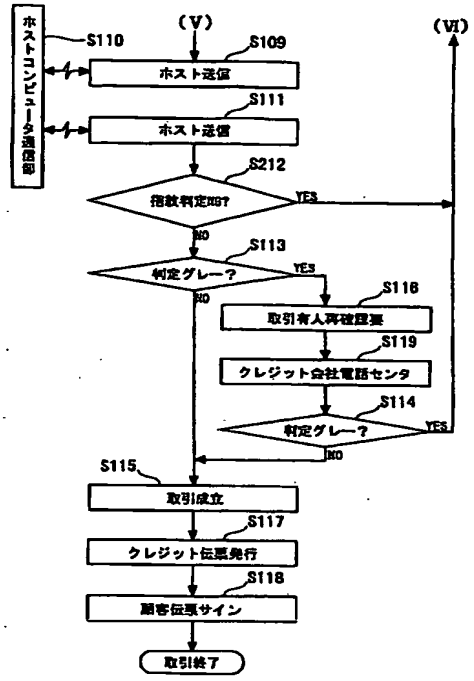
【図７】


ホストコンピュータ通信部
(Ⅲ)
S110
S109
ホストコンピュータに送信
S111
CATに送信
S112
CAT表示画面に表示された判定はNG?
YES
NO
S113
判定グレー?
YES
NO
S116
取引有人再確認
S119
クレジット会社電話センタ
S114
判定グレー?
YES
NO
(Ⅳ)
S115
取引成立
S117
クレジット伝票発行
S118
顧客伝票サイン
S120
取引終了

【図８】


S101
クレジット買物登録
S102
目視確認 カード写真＝本人顔?
NO
YES
S103
売上金額、支払回数等入力
S105
クレジットカード読取
S207
カード内指紋データ＝本人指紋?
NO
YES
S206
表示部に正規ユーザの指紋照合OK表示
S208
暗号化
(Ⅴ)
S104
事故カードによる取引中止（必要により警察へ届け出）
(Ⅵ)

【図９】



フロントページの続き

(51) Int. Cl.⁷		識別記号	FI		テーマコード（参考）
G06K	17/00		G06K	17/00	L 5J104
					T 5L096
					V
	19/00		G06T	1/00	340A
	19/10			7/00	300F
G06T	1/00	340	H04L	9/00	673D
	7/00	300	G06K	19/00	Q
G07F	7/12				S
H04L	9/32		G07F	7/08	B

Ｆターム(参考) 2C005 HA03 HB01 HB07 HB09 HB20
JA08 JB02 JB05 JB06 JB33
LA29 LB32 LB34 MA04 MB01
MB07 MB08 MB10 QC12 SA02
SA14 SA15 SA16
3E044 AA20 BA05 CA03 CA06 CA10
DA05 DA10 DD01 DE01 DE02
5B035 AA13 AA14 BB09 BB11 BC01
CA06 CA29
5B057 AA19 BA02 CA12 CA16 DA11
DB02 DC01 DC36
5B058 CA22 CA25 KA02 KA04 KA05
KA06 KA08 KA31 KA35 KA37
YA02
5J104 AA07 EA22 KA16 MA01 NA33
5L096 BA03 BA18 CA02 FA00 JA11